Anonymity in Tor-like systems under Timing Analysis: An Information Theoretic Perspective

Parv Venkitasubramaniam

"Tor does not provide protection against end-to-end timing attacks: If your attacker can watch the traffic coming out of your computer, and also the traffic arriving at your chosen destination, he can use statistical analysis to discover that they are part of the same circuit" - http://www.torproject.org. Indeed, as first demonstrated in [1] and bolstered by many follow up studies since, timing attacks have continued to be a significant threat to anonymity in a Tor-like system. While timing attacks are only a subset of possible attacks on an anonymous system, resilience to timing attacks can be studied from an independent perspective. Protection of anonymity from timing analysis requires characterizing the *information* retrievable from timing, and consequently designing packet scheduling protocols for mixes that minimize this information. This paper provides an information theoretic perspective on the study and prevention of timing analysis, and briefly discusses the implications on the design of anonymous systems.

Consider a network of Mixes in a Tor-like system. Taking a conservative standpoint, assume that a powerful adversary has the ability to monitor the timing of packet transmissions on all links in the system. Such a worst case assumption will ensure that in most practical scenarios timing attacks will perform strictly worse than that theorized. In such a network of mixes, each mix typically employs protective measures such as layered encryption, packet padding to increase the sender anonymity of packets on any outgoing link. Prevention of timing based information retrieval necessitates that mixes selectively delay and reorder packets so as to decrease correlation between the timing of incoming and outgoing streams. The design and analysis of such delaying and reordering strategies necessitates three important characterizations:

- Prior Information available about the packet streams: Prior information may include likelihood of a source destination pair, likelihood of a timing pattern to arrive from a specific source or intended to a particular destination, knowledge of routing protocols and suchlike. Note that prior information necessarily includes only that which the reordering strategies cannot modify.
- *Complete* observation of an adversary during the functioning of the system. From the conservative standpoint, the complete observation of the adversary includes but is not limited to the timing of packet transmissions on all links of the network. Observation can also include additional information obtained by capturing/compromising mix nodes in the network.
- Formulating a metric that effectively quantifies the sender information retrievable using the prior information, complete observations made by an adversary, and *knowledge of the reordering strategy*. In this regard it is important to note two important caveats. First, the sender information that is retrievable does not lose value over time; the source of packets flowing into a destination at a given time can be retrieved by using all observations in the past, present and future. Second, no assumptions ought to be made on specific statistical tools used by an adversary to retrieve the information.

A metric thus formulated can then be used to evaluate and optimize the scheduling strategies of the mixes. While such an approach studies the prevention of timing analysis in isolation, the prior information characterization can be used to encapsulate information obtained through other kinds of attacks thus adapting the design process in a broader framework.

An inherent assumption in the discussion thus far is the passive nature of the adversary in merely monitoring the timing. If an adversary is capable of modifying the timing pattern of specific streams, the framework would be benefited by adopting a game theoretic perspective; network nodes design mixing strategies to minimize the information metric whereas the adversary designs timing modification strategies to maximize the information metric.

Shannon Theoretic Model for Sender Anonymity

The persisting conception of anonymity is that of being indistinguishable within a set. The specific notion of sender anonymity in effect refers to the inability of an adversary to accurately identify the sender of a packet or a stream of packets within a group of senders. A quantitative metric for sender anonymity should effectively measure this ability (or inability) given the complete knowledge of the adversary. In the context of timing analysis, such a metric, when formulated in accordance to the requirements specified in the previous section, would reflect the effectiveness of the designed mixing strategies. If a probabilistic model can be defined for the system dynamics, Shannon entropy is one such metric.

Specifically, say we wish to measure the sender anonymity of packets on a destination link. Without making observations, the prior information available to the adversary would result in an a probability distribution of each packet on the link belonging to a particular source. This prior distribution models the prior knowledge available to the adversary in so far as it is helpful in determining the sources of packets on the link. Any observations made by the adversary during the system operation can only better his ability to identify the sources of packets. Accordingly, the Shannon entropy of the prior probability distribution denotes the maximum achievable entropy by any strategy adopted in the network. Having observed

the timing of packet transmissions during the *entirety* of the system operation, the knowledge of the mixing strategy would result in a posterior distribution on the sources of packets. The entropy of this posterior distribution provides a useful measure of anonymity from timing analysis. If the probabilistic model of the system is accurate, then the normalized posterior entropy is a lower bound on the minimum achievable probability of error by any adversary trying to determine sources, regardless of the statistical methods used (See Fano's Inequality [2]).

The key challenge in using Shannon entropy is defining a probabilistic model for the system. In this regard, we separate two sources of randomness: randomness in available prior information, and randomness due to the mixing strategies. While the former is characterized empirically using statistical information which can be insufficient, the latter is an outcome of the design process and is known. In fact, the probabilistic model built into mixing strategies is determinate and known to the adversary; what's not known to the adversary is the realization of the randomness during the operation of the network which results in uncertainty from the adversary's perspective. For a specific operation of the network, if I_P denotes the available prior information, O denotes the complete observation, $X_1, \cdots, X_n$ represent the sources of packets on the destination link, then the Shannon entropy

$$\frac{1}{n} H(X_1, \cdots, X_n | I_P, O) \stackrel{\triangle}{=} A$$

measures the per packet uncertainty from the adversary's perspective where $H(\mathbf{X}|\mathbf{Y})$ for a pair of random vectors $\mathbf{X} \in \mathcal{X}, \mathbf{Y} \in \mathcal{Y}$ is given by:

$$H(\mathbf{X}|\mathbf{Y}) = \sum_{\mathbf{x},\mathbf{y} \in \mathcal{X} \times \mathcal{Y}} - \Pr\{\mathbf{X} = \mathbf{x} | \mathbf{Y} = \mathbf{y}\} \log \Pr\{\mathbf{X} = \mathbf{x} | \mathbf{Y} = \mathbf{y}\}.$$

If $A = 0$, then the adversary can perfectly determine the source of every outgoing packet. If $A = \log s$ where s is the total number of possible sources, then each packet is equally likely to have arrived from any one of the s sources. In general the ratio $\frac{A}{\log s}$ provides a lower bound on the adversary's probability of error in determining the sources. Note that the use of joint entropy and conditioning on the complete information captures the performance of the best possible adversary in this context. Further, note that the entropy is calculated using the posterior probability distribution obtained using the knowledge of the mixing strategy. For any mixing strategy and observations drawn from the network operation, the metric defined above is computable and reflects the ability of an adversary to identify the sources of packets on a destination link. The lack of accurate prior information would limit the efficacy of this metric; it would then be useful to identify worst case prior information to bound the performance of mixing strategies.

Using Entropy to Optimize Mixing Strategies and Performance Tradeoffs

Given the entropic measure of anonymity in the context of timing analysis, the goal is to design strategies for individual mixes that maximize the achieved entropy for every realization of the network operation. Since the source destination pairs or sender timing patterns are unknown at the time of design, a probabilistic model for these processes would facilitate the design process. Since combating timing analysis requires delaying and reordering, it is imperative that resource and performance constraints of the system are taken into consideration while designing mixing strategies. In this regard, recent work has demonstrated that for Poisson traffic models, mixing strategies can be optimized under constraints on latency [3], memory [4], and fairness [5]. In particular, these results demonstrate the significant improvement in achievable anonymity over previously known delaying and reordering strategies. Although Poisson models were used in these results, the analyses also provide broad inferences about a Tor-like system that hold for general traffic models:

- A fundamental tradeoff exists between anonymity and QoS metrics such as delay, throughput, memory utilization. A system with no resource or QoS constraints can achieve the maximum possible anonymity (equal to the entropy of the prior probability distribution).
- The anonymity achievable by a network of mixes is a linear functional of the anonymity achievable by individual mixes weighted by traffic rates. This result is useful to separate the design of delaying strategies of individual mixes and the higher layer routing protocols for a network of mixes.
- Shared randomness across mixes can strictly improve achievable anonymity.

The optimization approach used and the results delineated in the previous section are appropriate for short bursts of packets between source destination pairs and the metric would compute an average per packet measure. In systems where sources transmit long streams of packets to destination, as in a multimedia P2P file sharing system, the observation of the adversary as time progresses would eventually reveal the sources of packets arriving on a destination link. For such high traffic systems, allowing the mixes to supplement outgoing links with dummy transmissions is essential. Recent results demonstrate analytically that without adding or dropping packets, the source of any stream can be perfectly identified given enough time. The entropic approach for the anonymity measure can be used in such systems as well; the definition requires modelling the prior information about timing patterns to reflect the indefinite length of streams for the source destination pairs [6].

In conclusion, anonymity from timing analysis is essential to the design of Tor-like systems and Shannon entropy provides a useful measure to study the problem in isolation with a mechanism to combine with information from other attacks. Although it is not the only possible metric that captures the required characterizations, it has been demonstrably useful in designing scheduling strategies and deriving broad inferences about anonymity in networks of mixes. We do note that Shannon entropy computes an average over the probability distribution, and in certain situations, supplementing the metric with a min-entropy computation would evaluate the effectiveness of the measure.

REFERENCES

[1] Y. Zhu, X. Fu, B. Graham, R. Bettati, and W. Zhao, "On flow correlation attacks and countermeasures in mix networks," in *Privacy Enhancing Technologies*, pp. 207–225, Springer, 2005.

[2] T. M. Cover and J. A. Thomas, *Elements of information theory*. Wiley-interscience, 2012.

[3] P. Venkitasubramaniam and V. Anantharam, "Anonymity under light traffic conditions using a network of mixes," in *Communication, Control, and Computing, 2008 46th Annual Allerton Conference on*, pp. 1373–1380, IEEE, 2008.

[4] P. Venkitasubramaniam, "Anonymity under buffer constraints," in *IEEE International Conference on Communications*, 2010.

[5] A. Mishra and P. Venkitasubramaniam, "Source anonymity in fair scheduling: A case for the proportional method," in *Communications (ICC), 2012 IEEE International Conference on*, pp. 1118–1122, IEEE, 2012.

[6] P. Venkitasubramaniam and L. Tong, "Anonymous networking with minimum latency in multihop networks," in *Security and Privacy, 2008. SP 2008. IEEE Symposium on*, pp. 18–32, IEEE, 2008.